METHODOLOGIES FOR IMPLEMENTING BLOCKCHAIN IN NOVEL APPLICATION AREAS

A

SHORT SYNOPSIS

SUBMITTED TO

MANAV RACHNA UNIVERSITY

FOR THE DEGREE

OF

DOCTOR OF PHILOSOPHY

IN

DEPARTMENT OF COMPUTER SCIENCE AND TECHNOLOGY

By

Riya Sapra
2K18-PFE-002.

UNDER THE GUIDANCE OF

Dr. Parneeta Dhaliwal
Associate Professor, Department of Computer Science & Technology

MANAV RACHNA UNIVERSITY
Established, vide Haryana Act no.26 of 2014
(Formerly Manav Rachna College of Engineering,
NAAC Accredited 'A' Grade Institute)

2017-18

MANAV RACHNA UNIVERSITY

Established, vide Haryana Act no.26 of 2014
(Formerly Manav Rachna College of Engineering,
NAAC Accredited 'A' Grade Institute)

DECLARATION BY THE SCHOLAR

I declare that the Synopsis entitled **"Methodologies for implementing Blockchain in novel application areas"** is prepared under the supervision of Dr. Parneeta Dhaliwal submitted for the approval of Departmental Research Committee (DRC).

Signature of Supervisor *Signature of Scholar*

Contents

1. Introduction 5

2. Review of Literature 8

3. Motivation 11

4. Objectives 12

5. Methodology 13

6. RoadMap 14

References 15

List of Figures

Figure 1: Blockchain Structure..... ……..1
Figure 2: Merkle Root Hash generation ..... **Error! Bookmark not defined.**

1. Introduction

Blockchain is a distributed computing technology that uses the decades old technology of public ledgers and cryptography to provide a secure, immutable and chronological ledger of records. But it gained popularity only after the release of first cryptocurrency, Bitcoin [12]. After the release of Bitcoin, various cryptocurrencies came to market. At present there are more than 2800 cryptocurrencies [1] and the number is increasing at rapid pace. Apart from digital money ecosystem, blockchain is being used in various other domains to provide privacy and security.

Blockchain is a collection of blocks connected to each other via hash of previous block as shown in Figure 1. Every block contains transactions stored in chronological order. Transaction is meant for recording an event. In case of a financial application [2], exchange of any value or asset can be a transaction. In Internet of Things (IoT) [3], transfer of data can be a transaction. In case of a healthcare application [4], exchange of any information can be a transaction. Transaction can denote any financial transfer or any data transfer or event change depending on the type of platform or application. These transactions are stored after converting them its hashes using a hash algorithm. In blockchain, user identities are also converted into hashes which provides privacy and user anonymity to the blockchain network.

A block [5] in a blockchain network has two parts: block header and block body. Block header has four components as shown in Figure 1:

- **Merkle Root Hash**: Merkle root represents the block as it is the block's root hash. It is calculated by combining the hashes of all the transactions of the block, level by level as shown in Figure 2. Every transaction is stored as a hash in the block using cryptographic function. Now every two adjacent hashes are joined to form a single hash from two hashes. At each level, this process of joining hashes is done till merkle root i.e. root hash is evaluated.
- **Previous Root Hash**: All the blocks in blockchain are connected by storing root hash of previous block and hence form a chain of blocks.
- **Nonce**: Nonce is a number, mostly a 32 bit number. The value of nonce is found by the miner against a puzzle and target number.
- **Timestamp**: Timestamp defines the block creation time.

Block body consists of all the transactions with their timestamps. The transactions are performed by nodes in the blockchain network. Nodes can be defined as anyone involved

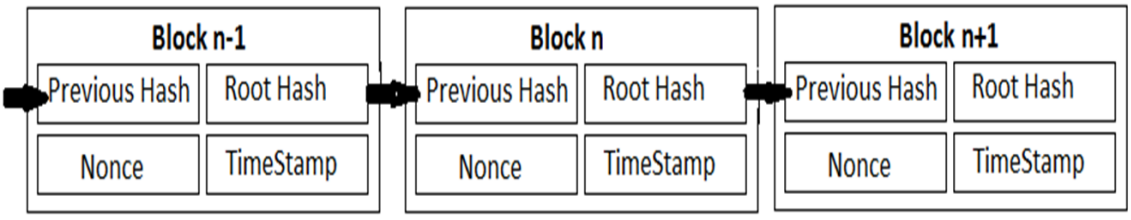

Figure 1. Blockchain Structure

in the blockchain network. He/She can send or receive transactions or can be a miner or might simply join the network to read transactions. Nodes can be distinguished in three categories depending on their task in the network:

Simple Node: Simple nodes only involve themselves in sending/receiving transactions. They are not involved in any validation or mining of blocks

Full Node: These are validator nodes of the blockchain network. They store a copy of blockchain to validate the transactions happening in the network.

Miner Node: Miner nodes are the working force of the blockchain network. They mine the transactions after validation from full nodes. They store the complete copy of the blockchain and create new block from the mined transactions. In blockchain, miner nodes have to compete within themselves to produce new blocks fast.

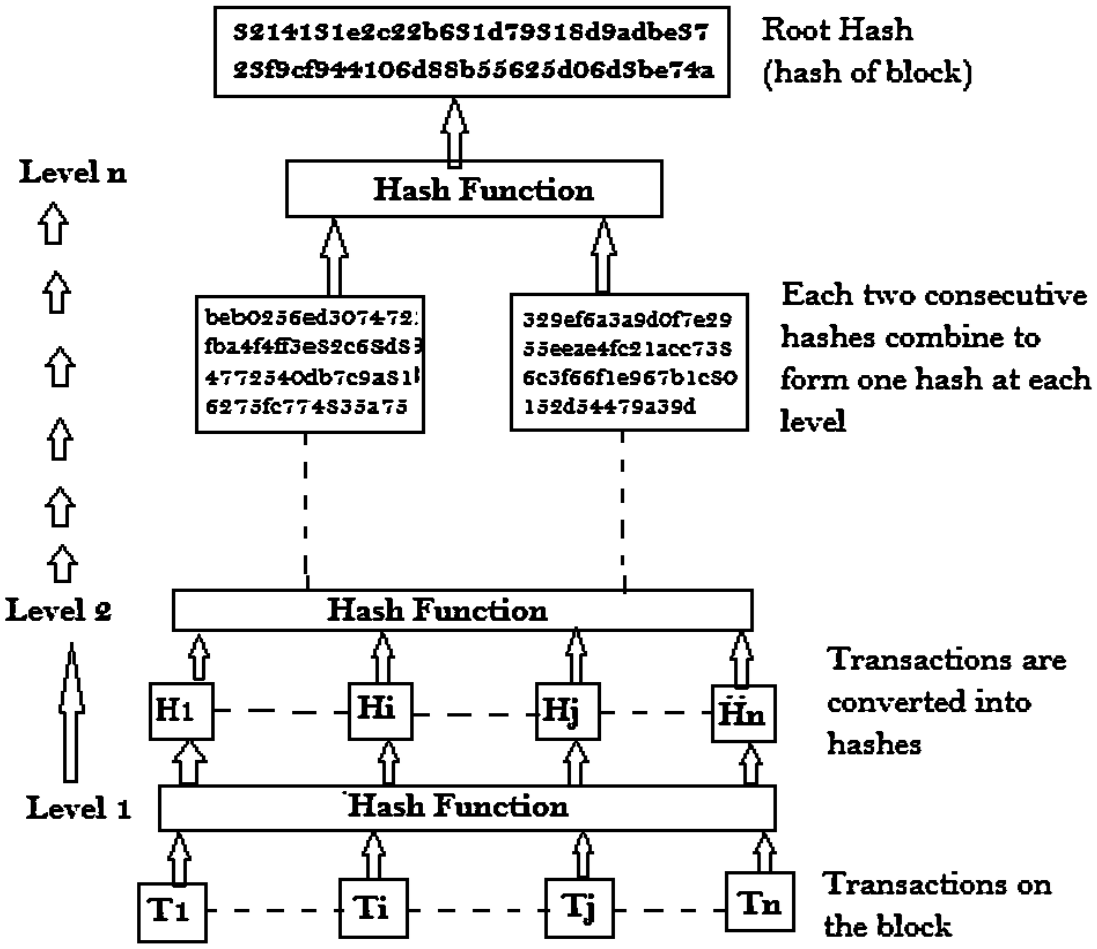

Figure 2: Merkle Root hash generation

The blocks are created using the process called mining. Transactions happen in real time. These transactions are broadcasted to every other node in the network. Various nodes validate the transactions. Miners convert transactions to hashes, find the root hash and nonce. Many miners are involved in mining process and compete among themselves to get their mined block appended to the blockchain.

There are three types of blockchain network according to the permission for nodes to read/write the transactions:

Public blockchain: Blockchain platforms like Dash [8], Bitcoin [12], Ethereum [6] etc. have transparent transactions. Anyone can join the network, read or execute transactions. Anyone can also audit the transactions without asking for any permission.

Federated Blockchain: These blockchain [7] are partially centralized blockchain. Permissions are required to join network, read or execute transactions. These blockchain networks don't permit everyone to audit the transactions. They are quicker than public blockchain and provide privacy. These blockchains area unit preferred within the banking sector. Corda [2] is a partly decentralized i.e. federated blockchain.

Private Blockchain: Private blockchain is more a centralized blockchain platform. Ripple [9] is one of the private blockchain. In this network, permissions to read or write permissions are solely designated to a private company or may be restricted to few licensed persons/ organizations. These blockchain networks are meant for sensitive information sharing.

2. Review of Literature

The concept of blockchain came from its first application Bitcoin [12]. Bitcoin is a cryptocurrency which uses PoW [12] consensus protocol for creation of blocks in blockchain. In PoW, nodes have to perform a difficult task using computing power to get their block appended to the blockchain. In PoW, large amount of power is wasted in calculation of nonce. Various other variants of PoW were also proposed to overcome this drawback of the algorithm. A variant of PoW is proposed which uses the Cuckoo hash function [10] in place of the complex task and uses fewer efforts by the miners to create a new block. Another variant uses a method of finding longest chain of primes larger than a specified given value to form a Cunningham chain [11]. These variants reduce the computing power and hence power wastage is reduced.

Proof of Stake [13] (PoS) is another consensus protocol that assigns miner on the basis of the stake available with the node. This ensures trust in the network as miner is the one with maximum stake at that point so he will not perform any fraudulent transaction to keep his/her stake safe. The blockchain platform, Nextcoin [23] uses pure PoS to select its miner. A miner pool is created on the basis of the stake they hold. A list of coin numbers these nodes hold is made. A random number is chosen from the list of coins and the node which owns that numbered coin is selected as miner. So the more coins a node has, more are his/her chances to be selected as a miner. PoS is faster than PoW and uses very less computation resources.

A variant of PoS uses coin flipping protocol to choose the miner. Another variant [14] chooses miners on the basis of the state of the block. Proof of Burn [15] is another consensus protocol where the nodes have to send their coins to some particular address, also called as burning of coins. The node who shares the most coins is selected as the miner for the block.

In Proof of space [16], plots are created and the nodes storing the most plots get to mine the block. Proof of elapsed time [17], every node who wants to be miner is given a random waiting time and the node with shortest waiting time is selected as miner. Proof of Luck [18] is another algorithm for creating blockchain on the basis of lucky numbers chosen by them. The miners keep on adding the blocks with their lucky numbers. The chain with highest total value is selected as the main blockchain.

Another consensus protocol Multichain [19] selects miner in a round robin fashion. Every node has a fair chance to be selected as miner. There are also few voting based consensus algorithms which might suffer from subversion or crashing of nodes. These algorithms are generally categorized as byzantine fault tolerant and crash fault tolerant algorithms. Byzantine fault tolerant algorithms include Practical byzantine fault tolerant (PBFT) [20], SMaRt [21], Sumeragi [22] etc.

PBFT [20] was first used by IBM in HyperLedger Fabric [23]. PBFT has two types of nodes: leader and peer. Leader node broadcast the proposed block in the blockchain network. Peer nodes crosscheck the proposed block and validate all the transaction in it. SMarT [21]

is similar to PBFT as it is also a Propose, write and accept consensus protocol like PBFT. In Sumeragi [11] consensus protocol arranges all nodes as a linear list, so as to reduce the broadcasting overheads. It then uses same procedure as PBFT to add new block.

Crash fault tolerant algorithms include Raft [25] and Federated [24]. Raft [25] assigns three different roles to the verifying nodes as leader, candidate and follower and uses RequestVote and AppendEntries as two message protocols for voting a leader node and transferring any request respectively. Whenever a transaction is made, it is sent to leader node. Leader node writes it to log entry and forwards it to the follower and candidate nodes to append entry of the transactions. These nodes verify the transactions and write them to block. The leader node verifies again and commits the block at last to the existing blockchain. Raft is being implemented in Quorum [27] blockchain platform.

Federated [24] is another crash tolerant consensus algorithm used by Ripple [26] blockchain platform. Nodes in federated consensus have two roles: block generators and block signers. Block generator receives transactions, verifies them and keep them in a temporary list. Block generator adds the verified transactions from temporary list to the block after a certain period of time and finally add it to the blockchain.

Apart from advances in consensus protocols, blockchain has evolved from mere a cryptocurrency to a technology which is being used in almost every emerging field of technology. It is also being used in a variety of application areas like healthcare [29-31], financial [33-35], property management [32], identity management [28] etc. In India, ICICI Bank [33] has started using blockchain for executing paperless transactions happening in India and abroad. Bajaj Finserv [33] also is using blockchain for claim settlement of travel insurance. Other financial applications include HomeSend [34], a blockchain based platform meant for cross border payments. Also Utility Settlement Coin (USC) [35] is a UK based blockchain project made for international banks to settle interbank payments by creating blockchain version of currencies: Euro, US dollar, British Pound, Canadian dollar and Japanese Yen.

In healthcare, many blockchain initiatives have started in last few years for facilitating doctors and patients to maintain and share health records data. Medrec [29], MedChain [30] and MedicalChain [31] are few blockchain platforms for storing the patient's medical records safely and sharing them if required. There are also other blockchain initiatives for managing user's identities. Estonia's e-residency [28] is a blockchain based platform where any person in the globe can become an e-resident after fulfilling certain conditions by Estonia and do business online. OneName [34] is another blockchain platform for digital verification of identities.

Blockchain is being used in other fields like retails [36], supply chain management [37], entertainment [38-40] etc. also. Loyyal [36] is blockchain loyalty platform which provides incentives to customers. Guts [38] is a blockchain platform for ticketing to remove frauds in the ticketing process. Matchpool [39] is a matchmaking blockchain platform to connect people of same community. Spotify [40] is a music blockchain platform which connects

artists with their license agreements. Corda [37] is blockchain based supply chain platform to connect suppliers and dealers on one platform to create a better ecosystem.

Blockchain has brought everyone to the era of smart contracts [41]. Various smart contracts platforms have been designed using the power of blockchain. Ethereum [41] being the first one to provide platform for smart contracts to build decentralized applications using it. Eris industries [42] and HyperLedger [43] are similar smart contract platforms to create decentralized applications. Bit & Coin AG [44] provide smart contract platform for energy suppliers. Slock it [45] is also a rental smart contract platform for renting real world objects. Block and Chain game studios [46] is another smart contract platform meant for gaming.

3. Motivation

- Smart contract is the next future.
- Smart contract can ease businesses via automatic transactions.
- Various applications have security and trust issues which can be solved using blockchain.
- Applications can be optimized using Blockchain for better process management.
- The data on blockchain can be accessed anytime and anywhere and is archived by various peers.
- Blockchain removes the problem of single point of failure.
- It can be used for applications where user identity needs to be hidden.

4. Objectives

- To develop blockchain platform for novel application areas.
- To use various hashing algorithms for encryption in blockchain.
- To propose new resource efficient algorithms for public blockchain.
- To resolve the security and trust issues of an application using blockchain.
- To create a new token or cryptocurrency using public blockchain.

5. Methodology

The proposed idea is to develop Blockchain systems for the existing as well as new application areas, providing security of data and privacy to the users without any third party interference. The concept of smart contracts will be used to automate various processes such as data transfers, payments etc. The applications may include:

- Organ Donation and retrieval
- Blood Donation and retrieval
- Criminal records
- Birth certificate generation
- Missing cases

Blockchain platform for these applications can be designed to reduce the manual tasks and delays occurring in the process. New resource efficient algorithms can be designed to optimize the blockchain system. A new hashing algorithm can be designed to optimize the process further. A new cryptocurrency can be proposed for any payment processing within the blockchain system.

Road Map

S.No.	Research Activities	Jan-Mar 18	Apr-Jun 18	Jul-Sep 18	Oct-Dec 18	Jan-Mar 19	Apr-Jun 19	Jul-Sep 19	Oct-Dec 19	Jan-Mar 20	Apr-Jun 20	Jul-Sep 20	Oct-Dec 20
1	Course Work												
2	Area Specific Course (Allocation and Completion)												
3	Literature Review												
4	Defining research problem												
5	Synopsis preparation												
6	Review paper writing												
7	Research paper submission/ publication in Conference												
8	Research paper submission in International Journal (Free)												
9	Learning of Tool												
10	Data Preparation												
11	Developing Algorithm												
12	Result Analysis												
13	Conference Paper writing and submission												
14	Research paper submission in International Journal (Free)												
15	Thesis Writing and Submission												

References

[1] Coinlore. (2019). Cryptocurrency List. Retreived on 20 -09-2019 from https://www.coinlore.com/all_coins

[2] Brown, R.G., Carlyle, J., Grigg, I. and Hearn, M., 2016. Corda: an introduction. R3 CEV, August.

[3] Kasturi, K., Reddy, P.V., Rao, N.A. and Vinod, S., 2016. A review of architecture and applications for internet of things. Advances in Natural and Applied Sciences, 10(9 SE), pp.261-267

[4] Rouhani, S., Butterworth, L., Simmons, A.D., Humphery, D.G. and Deters, R., 2019. MediChainTM: A Secure Decentralized Medical Data Asset Management System. arXiv preprint arXiv:1901.10645.

[5] Niranjanamurthy, M., B. N. Nithya, and S. Jagannatha. "Analysis of blockchain technology: pros, cons and SWOT." Cluster Computing (2018): 1-15.

[6] Ethereum Team. Ethereum White Paper—"A Next-Generation Smart Contract and Decentralized Application Platform". Available online: https://github.com/ethereum/wiki/wiki/White-Paper (accessed on 29 December 2017).

[7] Sheetal, Ms, and K. A. Venkatesh. "Necessary requirements for Blockchain Technology and its Applications." (2018).

[8] Duffield, E., Diaz, D. "Dash: A Privacy-Centric Crypto-Currency." No Publisher (2015) https://www.dash.org/wp-content/uploads/2015/04/Dash-WhitepaperV1.pdf.

[9] Olleros, F. Xavier, and Majlinda Zhegu, eds. Research handbook on digital transformations. Edward Elgar Publishing, 2016.

[10] Nguyen, G. T., & Kim, K. (2018). A Survey about Consensus Algorithms Used in Blockchain. Journal of Information Processing Systems, 14(1).

[11] C. K. Caldwell, "Cunningham chain," 2017 [Online]. Available: http://primes.utm.edu/glossary/xpage/CunninghamChain.html.

[12] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.

[13] King, S., & Nadal, S. (2012). Ppcoin: Peer-to-peer crypto-currency with proof-of-stake. self-published paper, August, 19.

[14] I. Bentov, A. Gabizon, and A. Mizrahi, "Cryptocurrencies without proof of work," in Financial Cryptography and Data Security. Heidelberg: Springer, 2016, pp. 142-157.

[15] Li, W., Andreina, S., Bohli, J. M., & Karame, G. (2017). Securing proof-of-stake blockchain protocols. In Data Privacy Management, Cryptocurrencies and Blockchain Technology (pp. 297-315). Springer, Cham.

[16] Dziembowski, S., Faust, S., Kolmogorov, V., & Pietrzak, K. (2015, August). Proofs of space. In Annual Cryptology Conference (pp. 585-605). Springer, Berlin, Heidelberg.

[17] Chen, L., Xu, L., Shah, N., Gao, Z., Lu, Y., & Shi, W. (2017, November). On security analysis of proof-of-elapsed-time (poet). In International Symposium on Stabilization, Safety, and Security of Distributed Systems (pp. 282-297). Springer, Cham.

[18] Milutinovic, M., He, W., Wu, H., & Kanwal, M. (2016, December). Proof of luck: An efficient blockchain consensus protocol. In Proceedings of the 1st Workshop on System Software for Trusted Execution (p. 2). ACM

[19] G. Greenspan, "MultiChain Private Blockchain," 2015 [Online]. Available: https://www.multichain.com/download/MultiChain-White-Paper.pdf

[20] H. Sukhwani, J. M. Martinez, X. Chang, K. S. Trivedi, and A. Rindos, "Performance modeling of PBFT consensus process for permissioned blockchain network (Hyperledger Fabric)," in Proceedings of the IEEE 36th Symposium on Reliable Distributed Systems, Hong Kong, China, 2017, pp. 253-255.

[21] Cachin, C., & Vukolić, M. (2017). Blockchain consensus protocols in the wild. arXiv preprint arXiv:1707.01873.

[22] Saraf, C., & Sabadra, S. (2018, May). Blockchain platforms: A compendium. In 2018 IEEE International Conference on Innovative Research and Development (ICIRD) (pp. 1-6). IEEE.

[23] Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., & Muralidharan, S. (2018, April). Hyperledger fabric: a distributed operating system for permissioned blockchains. In Proceedings of the Thirteenth EuroSys Conference (p. 30). ACM.

[24] Innerbichler, J., & Damjanovic-Behrendt, V. (2018, June). Federated byzantine agreement to ensure trustworthiness of digital manufacturing platforms. In *Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems* (pp. 111-116). ACM.

[25] Huang, D., Ma, X., & Zhang, S. (2019). Performance analysis of the Raft consensus algorithm for private blockchains. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*.

[26] Baliga, A. (2017). Understanding blockchain consensus models. In *Persistent*.

[27] Morgan, J.P., 2016. Quorum whitepaper. New York: JP Morgan Chase.

[28] Sullivan, C. and Burger, E., 2017. E-residency and blockchain. computer law & security review, 33(4), pp.470-481.

[29] Azaria, A., Ekblaw, A., Vieira, T. and Lippman, A., 2016, August. Medrec: Using blockchain for medical data access and permission management. In 2016 2nd International Conference on Open and Big Data (OBD) (pp. 25-30). IEEE.
[30] Shen, B., Guo, J., & Yang, Y. (2019). MedChain: Efficient Healthcare Data Sharing via Blockchain. Applied Sciences, 9(6), 1207.
[31] https://medicalchain.com/en/
[32] Kshetri, N., & Voas, J. (2018). Blockchain in developing countries. It Professional, 20(2), 11-14.
[33] Sheetal, M., & Venkatesh, K. A. (2018). Necessary requirements for Blockchain Technology and its Applications, International Journal of Computing Science and Information Technology, 2018.
[34] Olleros, F.X. and Zhegu, M. eds., 2016. Research handbook on digital transformations. Edward Elgar Publishing.
[35] http://fortune.com/2017/08/31/banks-ubs-blockchain-settlements/
[36] https://loyyal.com/
[37] Brown, R.G., Carlyle, J., Grigg, I. and Hearn, M., 2016. Corda: an introduction. R3 CEV, August.
[38] https://guts.tickets/
[39] https://www.matchpool.com/
[40] https://www.spotify.com/
[41] Antonopoulos, A.M., 2014. Mastering Bitcoin: unlocking digital cryptocurrencies. " O'Reilly Media, Inc.".
[42] Mattila, J., 2016. The blockchain phenomenon. Berkeley Roundtable on the International Economy (BRIE), pp.2016-1
[43] Hyperledger Architecture, Volume II, Available at https://www.hyperledger.org/wp-content/uploads/2018/04/Hyperledger_Arch_WG_Paper_2_SmartContracts.pdf
[44] http://www.bit-coin.ag/
[45] Bahga, A. and Madisetti, V.K., 2016. Blockchain platform for industrial internet of things. Journal of Software Engineering and Applications, 9(10), p.533.
[46] Reyna, A., Martín, C., Chen, J., Soler, E. and Díaz, M., 2018. On blockchain and its integration with IoT. Challenges and opportunities. Future Generation Computer Systems, 88, pp.173-190.

Title of Research work: Methodologies for implementing Blockchain in novel Application Areas

Name of Scholar: Riya Sapra

Subject: Computer Science and Technology

Registration No: 2K18-PFE-002

Name of Guide: Dr. Parneeta Dhaliwal

Designation: Associate Professor

Guide working place: Manav Rachna University, Faridabad

MANAV RACHNA
Vidyanatariksha

Swami Vivekananda Library and Resource Centre
Manav Rachna University

SIMILARITY VERIFICATION CERTIFICATE

Title: Methodologies for implementing Blockchain in Novel Application Areas.

Researcher: Riya Sapra

Registration Number: 2K18-PFE-002

Supervisor: Dr. Parneeta Dhaliwal

Department: CST, MRV

This is to certify that the above mentioned Short Synopsis/~~Thesis~~ was scanned for similarity index through Turnitin Software on 20-11-19 with submission ID 1217832694 and the similarity index was found to be 10 %. The complete report running into 20 Pages, 2286 Word count with File Size 1949 KB is being forwarded to the Research Supervisor/DRC/DRB for review.

Date: 26 Nov 2019

Head, Libraries
Manav Rachna University
Faridabad, Haryana
Head, Libraries

The complete report of the above Short Synopsis/~~Thesis~~ has been reviewed and the similarity index is below the accepted norms as per the University Grants Commission (Promotion of Academic Integrity and Prevention of Plagiarism in Higher Educational Institutions) Regulations 2018. The Short Synopsis/~~Thesis~~ may be considered for further processing

Riya 26/11
Research Scholar

Parneeta
Research Supervisor

SYNOPSIS Riya Sapra NOV.20,2019

by Riya Sapra 1

Submission date: 20-Nov-2019 05:26PM (UTC+0530)
Submission ID: 1217832694
File name: synopsis_Riya_Sapra_nov.20,2019.docx (443.85K)
Word count: 2286
Character count: 12233

SYNOPSIS Riya Sapra NOV.20,2019

ORIGINALITY REPORT

10%	0%	8%	7%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

26/XI/19

Head, Libraries
Manav Rachna University
Faridabad, Haryana

1	"Principles of Internet of Things (IoT) Ecosystem: Insight Paradigm", Springer Science and Business Media LLC, 2020 Publication	6%
2	Riya Sapra, Parneeta Dhaliwal. "Blockchain: The new era of Technology", 2018 Fifth International Conference on Parallel, Distributed and Grid Computing (PDGC), 2018 Publication	1%
3	Submitted to Dublin City University Student Paper	<1%
4	pintotours.net Internet Source	<1%
5	Submitted to Jaypee University of Information Technology Student Paper	<1%
6	Submitted to Girne American University Student Paper	<1%
7	Marianna Belotti, Nikola Bozic, Guy Pujolle,	<1%

	Stefano Secci. "A Vademecum on Blockchain Technologies: When, Which and How", IEEE Communications Surveys & Tutorials, 2019 Publication	
8	Mads Frederik Madsen, Mikkel Gaub, Malthe Ettrup Kirkbro, Soren Debois. "Transforming Byzantine Faults using a Trusted Execution Environment", 2019 15th European Dependable Computing Conference (EDCC), 2019 Publication	<1%
9	Submitted to University of Leeds Student Paper	<1%
10	Riya Sapra, Parneeta Dhaliwal. "Chapter 24 Blockchain for Security Issues of Internet of Things (IoT)", Springer Science and Business Media LLC, 2020 Publication	<1%

Exclude quotes	On	Exclude matches	Off
Exclude bibliography	On		